Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Analysis of Blinding Over Asymmetric Cryptosystems Technique of Cryptography

Deepika Arora*
M.C.A
SITE,VIT University
Vellore (Tamil Nadu), India

Varun Kumar.M
Assistant Professor
SITE,VIT University
Vellore (Tamil Nadu), India

Abstract: Day to day internet users visits a number of sites depends on Hyper Text transfer Protocol for unbroken communication with the sites they designed to visit. From Last few Years, attackers attack on the system or network to fetch the unauthorized information. To make the information more secure from unauthorized access, protection must be provided to the information over the network. The purpose of computer networking brings a huge transformation in behavior to access the information. Now the information is spread over the network. The information must be secure and confidential when it is save in a system or when it is send from one system to another system, so the unauthorized user can not access the information. The main two approaches play a vital role to make the information more secure and provides confidentiality-One is steganography and the second is cryptography. It has been tried a number of attacks to break the security while working with these techniques. The basic idea of the paper is to transform the attack, i.e. based on key generation using an approach of Blinding over asymmetric cryptosystem technique for security purpose.

Keywords:

I. INTRODUCTION

There are basic three security procedures used to achieve the security of information-integrity, confidentiality and availability. Cryptography is a basic approach to provide security and confidentiality over unreliable network. Cryptography is a science i.e. holds the procedure to transfer the reliable information into unintelligible form, and unintelligible information back to its original manner with security. Cryptosystem is a pair of algorithms that receive a key and transform the plaintext to cipher text. There are mainly two type of cryptosystem is used- one is asymmetric cryptosystems and other is symmetric cryptosystems. Encryption and Decryption uses single key in Symmetric Cryptosystem. Where as in Asymmetric Cryptosystems two keys are used –private and public key. Public key is used to encrypt the information and private key is used for decryption.RSA Cryptosystem is a general public key algorithm used for security purpose. Several attacks have been tried on RSA Cryptosystems but all are failure .In this paper I tried to evaluate one another attack known as Blinding over RSA cryptosystems. Blinding is an approach to get a paper signed without showing the main subject of the message information to the signer. There are basically three steps are used to follow this technique:

1- The dispatcher create the significance message and blinds it, Receiver receives the blinded message from the sender.

2- The significance blinded message is signed by the receiver and give it back its sign on the significance blinded message.

3- On the original significance message, sender un blinds the signature to get the signature.

II. OBJECTIVE

The main purpose of this paper is to assess the technique of blinding attack over asymmetric RSA cryptosystem. Here I have tried to estimate how the signature of a person can get by the other person on any paper .To provide security and confidentiality from unauthorized access key generation over RSA Asymmetric Cryptosystem technique is used.

III. LITERATURE REVIEW

R.L.Rivest et al. [1] has illustrated that fake signature approach and a partially fake signature approach is depending upon the basic approach. Thus RSA assumption was mainly proposed for fake signature and a partially fake signature approach.

Dejian Fang et al. [2] has mentioned the elimination of the vulnerability of the last version to map out the attack. He tried to correct Chein's Digital signature or Blind signature approach depend on RSA Cryptosystems.

Diffie and Hellman et al. [3] has invented the difficulty to sort out the problem of non-traceability or blind signature. Here the sender encrypts the data before receiving by the receiver. No unauthorized person knows the decrypted message to obtain the original information.

IV. PROBLEM DEFINITION

A big problem in the area of Cryptography is to provide the security and confidentiality of information from unauthorized person in such a manner i.e. that information must be secured from all unauthorized access. A number of attackers have been tried to attack on the encrypted data. Therefore to get away from various attacks I tried to Blinding over RSA Cryptosystem using key generation.

V. EXPERIMENTATION, ANALYSIS AND MODELLING

There are two keys used in asymmetric cryptosystems- public key is used to encrypt the data and private key is used to decrypt the data. Some mathematical notations are used over the numbers under encryption and decryption to represent the plaintext and cipher text respectively. The cipher text, C = f (K_{PU} , M) can be generated using the given function and similarly the plain text can be generated using the function M = g ($K_{PR,}$ C).Here the functions f and g are used for encryption and decryption the message or information. Trapdoor one way function is the main idea of the asymmetric cryptosystem.

The notation e as the public key and d as the private key are used in RSA cryptosystems. Let us assume M_t and C_t are the plain text and cipher text respectively. The sender uses e as the public key to generate the cipher text C_t of the receiver from the plain text M_t by the notation $C_t=M_t$^e mod n; and receiver uses d as the public key to attain the plain text M_t from the cipher text C_t using the notation $M_t=C_t$^d mod n ; Where n is a modulus of a large prime number generated during the key generation process.

Fig: 1- The RSA cryptosystem

A. Blind Signature Scheme

The RSA scheme when used to realize digital signatures reverses the role of public and private key. Here the private key of the sender is used to provide the signatures on the documents. On the other side i.e. destination, public key of the sender is used to verify the signature. Thus we can conclude that the private key of the sender correspond to his signature with public key corresponding to the copy of the signature.

Digital signatures can also be implemented by RSA approach .It is also known as RSA digital signature scheme. In this scheme the job of private and public keys are different.

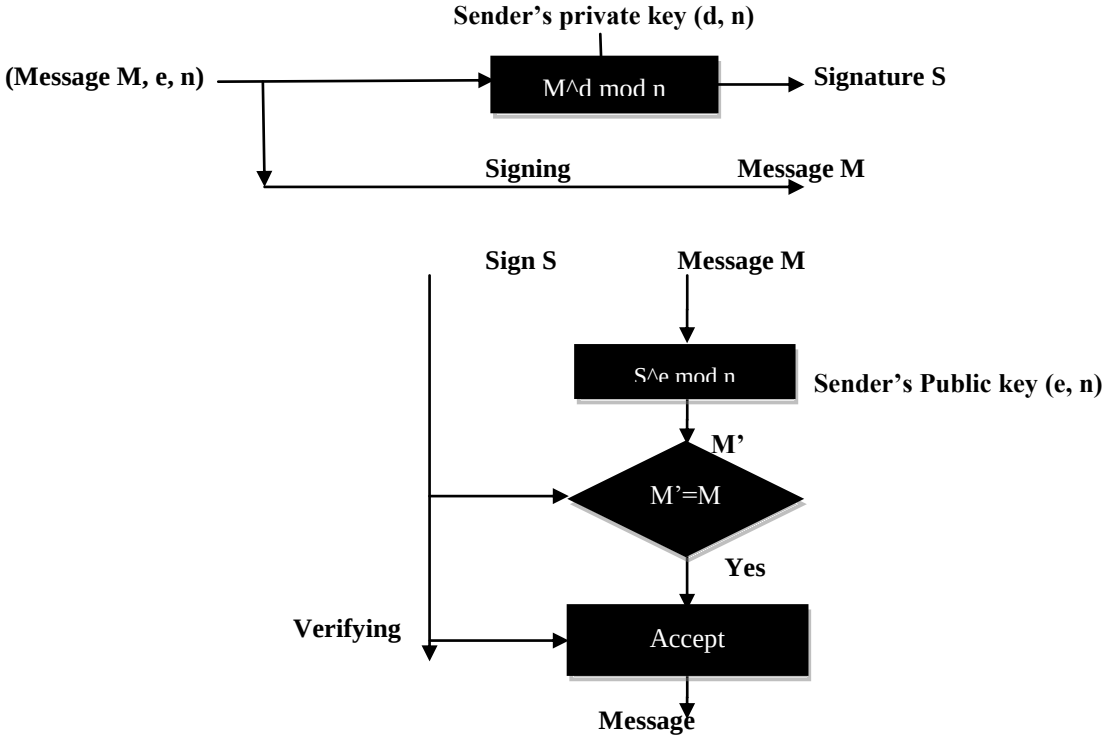

Fig: 2- The RSA digital signature scheme

B. Signing

The sender signs his document from the message by using his private exponent notation $S_g=M_t\text{^}d \bmod n$ and receiver receives the same message along with signature on a document.

C. Verification

The original signatures from sender are matched against the ones computed at the receiver side. If matches both the signatures, then the document is accepted. The signature computed on the receiver side is known as a copy of the original document. Destination side computes this copy by applying public exponents of the sender to the signature of the sender. This given fact is proved as follows:

$M^c = M \bmod n \rightarrow S^e = M \bmod n \rightarrow M^{e*d} = M \bmod n$

There have been many attackers tried of attacks on the RSA Signature approach i.e. Blind signature attacks, Key only attack and chosen message attack. The main idea behind this paper is to explore the attack known as Blinding over RSA digital signature scheme.

D. Blind Signatures

The sender with evil intentions can obtain the signatures of the receiver on some documents without him knowing about the real content of the message. Blind signatures derived by David Chaum served this purpose. The Blind signatures are conceptualized as follows:

1) The sender blinds the message by encapsulating it within a blind message.
2) The receiver just able to discover the blind message finds it safe enough to provide his signatures on it, thereby signing a blinded message.
3) The sender then removes the blind message segment and thereby obtains the signature on the intended message.

Let us discuss the working of the blinding scheme proposed by David Chaum. The sender blinds the message by raising product of the message and a randomly selected number r also called as blinding factor to the power of the receiver's public key ($B^M = (M * r)^e \, mod \, n$). The receiver sees a blind message and provides his signature as $Sb = B^{M^d} \bmod n$ using his private key d. The sender can now just perform he multiplicative inverse of the blinding factor r to remove the encapsulating blind message.

$S = Sb * r^{-1} \rightarrow B^{M^d} * r^{-1} \rightarrow ((M * r^e)^d) * r^{-1} \rightarrow (M^d) * r^{ed} * r^{-1} \rightarrow M^d * r * r^{-1} \rightarrow M^d$.

E. Proposed Work

In our proposed scheme we are going to have a global key pair that can perform encryption and decryption message sent to and from other participants. A participant's message encrypted using his secret key can be decrypted by the public key of the global key pair. The participant can decrypt the messages (encrypted with the global secret key) using its secret key. For example, there are n participants, there must be n pairs of public and secret keys $((e_1, d_1),(e_2, d_2),(e_3, d_3)\ldots(e_n, d_n))$, such that each $e_i * d = 1 \bmod L_i$, where L_i is the LCM of p_i -1 and q_i- 1 with public $n_i (n_i = p_i q_i)$. The global key pair shall also satisfy the condition such that $\boldsymbol{e_h * d_h = 1 \bmod L}$, with L computed as the LCM of $L_1, L_2, \ldots, L_n$.

The three phases included in the proposed scheme are:

(1) **Initialization:** this phase consists of generating the pairs of secret keys. Public data comprising of the master encrypting key (e_1, n). Private data are the moduli $(n_1, n_2, \ldots n_n)$ along with the respective secret keys $d_1, d_2, \ldots, d_n$.

(2) The steps involved are:

1) n public key pairs of RSA are generated.
2) The master key pair of the *n* key pairs within *n* time intervals is generated using koyama's algorithm.
3) The keys are ordered as per the suffix with respect to time intervals in the ascending order.
4) master key to encrypt are announced(e_i, n)
5) Respected keys are published in their respective time interval.

(3) **Signing phase in time interval i:** The module n_i is announced by the signer. Signature seekers shall use the key e_1,n (master encryption key pair) along with the module n_i to obtain a blind signature. The procedure is as-

$\alpha = r^{(e_i,n)} * h(M) \bmod n_i$

$S' = \alpha * d_i = (r^{(e_i,n)} * h(M))^{(d_i)} \bmod n_i = r(h(M))^{(d_i)} \bmod n_i$,

there by transmitting t to the seeker.

The signature seeker calculates-

$S = r^{(-1)} * S' \bmod n_i = r^{(-1)} * r(h(M))^{(d_i)} \bmod = n_i = (h(M)^{(d_i)}) \bmod n_i$

Here they obtained two tuples (M, S) is the signature of the signer over the message M.

(4)**Verification phase in time interval *i*: The verification requires e_1,*n* and n_i to verify the signature (S,M) where *S* = *h*(*M*) d_i *mod* n_i.**

1. first parameter v_1 is calculated as $v_1 = h(M) \ mod \ n_i$.
2. second parameter v_2 is calculated as $v_2 = S^{(e_1,n)} \text{mod } n_i$.
3. The two parameters are tested for being equivalent.

F. Fraud Avoidance

A useful scheme like blinding should be prevented from being used unethically. To protect the misuse-

1) The signing person as the laws from the regulating authorities shall never be responsible for signing any such document against his good.
2) The signer shall seek for the agreement that nothing would go against him.
3) The sender could be expected to prove his honesty before obtaining the signer's signature on the document.

VI. RESULT AND DISUSSIONS

Analyses can be made in two ways: (1) In the exact time period i_e , the correct information $(m_e)^{\wedge}d_i$ modulus n_i of the message m_e can be get by requesters.(2) In the last time period requesters cannot get valid signatures directly. Let's assume e1 is the encryption key for k periods. Then encryption master key e1 used by the requesters, in k time periods. The decryption keys are altered at various different time periods, to the signer. During the time period i, the signer use the notations d_i and n_i to the signed document. The notation m_e is $(m_e)^{\wedge}d_i$ mod n_i is used as a signature of the message. The approach of blindness ensures that the message information $m_{e\ is}$ unknown to the signer in the signing segment.
Although the signing segment is depend on RSA digital signature scheme, The random number r_e also provides "protection" to the message m_e .The only part of the message signer knows is temporary variable C1, where $C1 = r^{\wedge}(e1,k)*(m_e) \text{ mod } n_i$ but not the whole message m_e . C1 cannot be factories by the signer to obtain the message m because r is unknown to him.

VII. CONCLUSION AND FUTURE WORK

The basic idea of this paper is to estimate the attack of the Blinding technique .Here I have tried to propose how others signature can get directly through Blinding on the document without showing the matter of the paper. Thus it is applicable in various banking applications i.e.-commerce to virtual memory. While a number of attacker tried to attack on Blinding technique over RSA cryptosystem but none of them overwhelming to crack the algorithm.

REFERENCES

[1]. A blind signature scheme based on elgamal- Elsayed Mohammed, A.E.Emarah and Kh.El-Shennawy.
[2]. "On blind signature and perfect crimes" ,In Computers and security- B.von Soims and D.Naccache.
[3]. An Enhanced RSA-based Partially Blind Signature – Dejjan Fang, Na Wang,Chenglian Liu.
[4]. Security of blind digital signature technique- A juels M Luby,and R Ostroysky.
[5]. A strong RSA Signature Scheme and its Application- Zhengjum Cao,Lihua Liu.
[6]. Blind signatures for untraceable payments- R.L.Rivest,A.Sheman,and D.Chaum

